DELAWARE DEPARTMENT OF TECHNOLOGY & INFORMATION

December 2008 Issue

SECURITY - Now ...more than ever!

Cyber Security - Disaster Recovery - Continuity of Government

DTI eSecurity News - Smart Internet Shopping

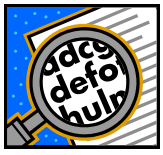
Shop Smart! Avoid Scams!

The holidays are approaching, and more people will be shopping online. While brick and mortar stores allow us to see and touch items before buying them, online shopping can actually provide for safer and smarter shopping. There are no crowds to contend with, online discounts are available, financial transactions can be more secure, and your personal safety is ensured when shopping after dark.

Following certain precautions can make your online shopping experience less stressful and more secure.

- **Know who you are doing business with before placing an order.** Confirm the seller's physical address and phone number in case there are questions or problems.
- **Limit online shopping to merchants you know and trust.** Merchants can be verified with the Delaware Better Business Bureau.

- **Know exactly what is being purchased.** Words like "refurbished", "vintage", or "close-out" may indicate that the product is in less-than-mint condition, while name-brand items with "too good to be true" prices could be counterfeits.
- **Phone-In Option.** Many web merchants allow you to order online and give your credit card information over the phone. If you do this, make a note of the phone number, company, the date and time of your call, and the name of the person who recorded your credit card number.
- **Get the details before ordering.** Check delivery dates, shipping and handling fees, warranties, and return policies. This might save you from future aggravation and communication with the merchant.



- **Keep a paper trail.** Print and save records of online transactions, including the product description and price, the online receipt, and copies of every email sent to the seller or received from the seller. *Read credit card statements as they are received, and be on the lookout for unauthorized charges.*

Questions or comments?
E-mail us at eSecurity@state.de.us

Protect Yourself

- **Third Party Seals of Approval.** Companies can put these seals on their sites if they abide by a set of rigorous standards - such as how complaints and disputes will be resolved and how personal information can be used. If you do see the seals, click on them to make sure that they link to the organization that created them. Some unscrupulous merchants will put these logos on their sites without permission, and they're less likely to get caught if they don't link back to the site.

- **Debit card transactions may not be protected, so pay by credit card.** If using a credit card to pay online, the transaction will be protected by the Fair Credit Billing Act. Also, check to see if your credit card company offers "virtual" account numbers - one-use account numbers, for online purchases, that are tied to your real account number.

- **Never email financial information.** Email is not a secure method of transmitting financial information, like credit card number, checking account number, or Social Security number.
- **Make sure your transactions are secure.** If a transaction is initiated, and financial information is provided through an organization's website, look for indicators that the site is secure; like a lock icon on the browser's status bar or a URL for a website that begins with "https" (the "s" stands for "secure"). Unfortunately, no indicator is foolproof; some fraudulent sites have forged security credentials.

If You've Been a Victim...

If there are problems during a transaction, try to work them out directly with the seller, buyer, or site operator. If that doesn't work, file a complaint with:

- The Attorney General's Consumer Protection Office.
- The Delaware Better Business Bureau.
- The Federal Trade Commission.

Produced in part by US-CERT

Visit the eSecurity Extranet website for previous issues of eSecurity Newsletters